

**STATEMENT OF GREGORY H. FRIEDMAN
INSPECTOR GENERAL
U. S. DEPARTMENT OF ENERGY**

BEFORE THE
U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS

FOR RELEASE ON DELIVERY
Tuesday, July 26, 2005

Good morning Mr. Chairman and members of the Subcommittee. I am pleased to be here at your request to testify on the readiness of the Department of Energy's energy, science, and environment sites to successfully defend against the terrorist threat identified in the Department's October 2004 Design Basis Threat document.

Since 1997, the Office of Inspector General has reported security as one of the Department of Energy's most significant management challenges. This was based on the body of work that we have done in this area, the sensitivity of the Department's operations, and evolving threat assessments. Consequently, the Office of Inspector General devotes a significant portion of its resources to reviewing the effectiveness of security programs and operations at Department of Energy facilities. The result has been numerous findings and recommendations designed to enhance Department security.

I would like to highlight several recent Inspector General reports that address current security issues, including:

- protective force training and management,
- facility access controls,
- physical security,
- cyber security,
- protective force performance testing, and
- protective force communications.

A number of our issues parallel those addressed in the July 2005 draft Government Accountability Office report on protective forces at the Department's energy, science, and environment sites.

The Department's Basic Protective Force Training Program

The Department's contractors employed over 4,100 security officers responsible for protecting Department sites. Of this number, approximately 1,650 security officers served at energy, science, and environment sites.

The Department's policy is to train its security forces to deal with a broad range of threats and ensure interoperability across the complex. In March 2004, we completed a review to determine whether sites were meeting the requirements of the Department's standardized, basic protective force core training curriculum. In our report, "The Department's Basic Protective Force Training Program" (DOE/IG-0641), we noted that 10 of the 12 sites we reviewed had made significant modifications to the Department's established protective force core curriculum. Five of the 10 sites were energy, science, and environment facilities that store or had stored special nuclear material. Specifically:

- Each of the 10 sites eliminated or modified 2 or more blocks of instruction from the core curriculum;
- Seven sites reduced the intensity of hands-on training for skills that some security experts characterized as critical, such as handcuffing, hand-to-hand combat, and vehicle assaults; and

- None of the 10 sites included instruction in rappelling, which is a core curriculum course for special response team training.

We noted that some modifications occurred because site security managers questioned the applicability of certain courses or had related safety concerns. These modifications were not always detected or their impact on readiness assessed by the respective program offices or the Office of Security because the Department did not require sites to report changes made to the core training requirements.

The high number of modifications to the protective force core curriculum raised questions about the validity of the curriculum and may lead to an increase in the risk that the Department's protective forces will not be fully trained to carry out their security responsibilities.

Management concurred with our recommendations to review curriculum modifications and agreed to issue additional guidance defining when the Department should be notified about modifications.

Protective Force Training at the Department of Energy's Oak Ridge Reservation

In June 2005, we issued a report on "Protective Force Training at the Department of Energy's Oak Ridge Reservation" (DOE/IG-0694). We determined that contractor protective force personnel spent, on average, about 40 percent less time on combat

readiness refresher training than that specified in the training plan approved by Federal site managers. This included training in areas such as team tactical exercises, chemical and biological warfare, vehicle assault, handgun malfunctions, and the use of force.

We also found that protective force personnel worked in excess of 60 hours per week, despite a 60-hour maximum threshold for safe operations established in the Department's Protective Force Program Manual. In particular, protective force personnel at the Y-12 National Security Complex routinely worked in excess of 60 hours per week.

Management, in concurring with the report's findings and recommendations, stated that it intended to review the adequacy of protective force refresher training at Department sites, as well as the acceptability of deviations from the annual training plans for core protective force skills. Management also stated that the reduction of overtime continues to be a significant goal at Oak Ridge.

Management of the Department's Protective Forces

In June 2003, we raised training and overtime concerns in a report on the "Management of the Department's Protective Forces" (DOE/IG-0602). To the Department's credit, we found that in the post-September 11, 2001, period, improvements had been made in the management of its protective force program. However, we noted that the Department faced a number of challenges that could adversely affect the program. Specifically, we reviewed five sites, and we observed:

- Significant increases in unscheduled protective force overtime;
- Protective force morale and retention problems based on mandatory overtime and reduced training opportunities; and
- Long delays associated with granting clearances for newly employed protective force officers.

In the report, we recognized that the Department of Energy, like other Government agencies, faced security challenges relative to the unanticipated demand for additional security personnel immediately after September 11, 2001. We concluded, however, that in subsequent years, the Department had the opportunity to improve the operation of its protective force program by taking advantage of accelerated methods of processing security clearances for officers, incorporating specific performance metrics into protective force contracts, and developing an overall protective force contingency strategy.

In responding to the report, Department management stated that it had launched an initiative to enhance protective force management, including the use of expedited processing of security clearances for protective force personnel.

Security Access Controls at the Y-12 National Security Complex

In June 2005, we completed a review of an allegation that non-U.S. citizens were improperly allowed access to a leased facility at the Department's Y-12 National Security

Complex, which is an integral component of the Department's nuclear weapons program. In a report on "Security Access Controls at the Y-12 National Security Complex" (DOE/IG-0691), we found that foreign construction workers used false identification documents, which resulted in their gaining access to Y-12 facilities.

During our review, management at Y-12 issued a revised access policy. Nevertheless, we were concerned that similar findings may exist at other sensitive Department sites. Therefore, we recommended that management determine whether Department-wide actions were warranted. In response, management stated that future security inspections of Department facilities will include reviews of access control procedures.

Review of Security at the Strategic Petroleum Reserve

The Strategic Petroleum Reserve serves as the Nation's first line of defense against an interruption in petroleum supplies. The Reserve contains approximately 695 million barrels of oil valued at about \$36 billion.

In our June 2005 report on "Review of Security at the Strategic Petroleum Reserve" (DOE/IG-0693), we concluded that additional measures could be implemented to improve physical security at Reserve sites. Management agreed with our findings and recommendations and agreed to implement corrective actions. Specifically, we found that:

- The level of protection against the "insider threat" at the sites may not be consistent with the designation of the Reserve as part of the Department's

critical infrastructure. Of the non-protective force contractor employees at the Reserve, 87 percent had never been processed for any level of security clearance. Some of these employees were allowed unescorted access to sensitive areas.

- Similarly, the Reserve's deadly force policy may not be consistent with the Reserve's critical infrastructure designation.
- Finally, opportunities existed to make protective force performance tests at the Reserve more realistic. Specifically, we found that the Reserve's security condition threat level is often elevated for certain tests, which provides for additional protective force personnel to defend the site during the tests.

This performance test finding was similar to the findings of a January 2004 review at the Oak Ridge Reservation, where we found that: (1) a performance test at Y-12 was compromised as a result of certain protective force personnel being allowed to view computer simulations of the test scenarios prior to the test; and (2) there was a pattern of actions by Reservation security personnel going back to the mid-1980's that may have negatively affected the reliability of site performance tests.

The Department's Unclassified Cyber Security Program

In Fiscal Year 2004, the Department spent about \$2.6 billion on information technology to support its various missions. As required by the *Federal Information Security Management Act*, the Office of Inspector General conducts an annual independent

evaluation to determine whether the Department's unclassified cyber security program adequately protected data and information systems.

In our September 2004 report on cyber security, "The Department's Unclassified Cyber Security Program - 2004" (DOE/IG-0662), we found that the Department had initiated new policies that emphasized a risk-based approach to managing security that, when fully implemented, should strengthen cyber security across the Department. While these actions were commendable, problems continued to exist that could expose critical systems to compromise. Specifically, the Department had not:

- Completed certification and accreditation of each major system, to identify and mitigate risks;
- Prepared contingency plans to ensure that mission critical systems could continue or resume operations in the event of an emergency or disaster; and
- Taken action to ensure adequate security controls were in place at all sites.

Management concurred with our recommendations and informed us it is conducting a follow-on review of the Department's unclassified cyber security program.

Management of Oak Ridge Radio Projects

Department of Energy sites rely heavily on radio communications to support activities such as site emergency response, physical security, and protection. In its July 2005 draft report on the readiness of the Department's protective forces, the Government

Accountability Office stated that protective force officers at each of the five sites it visited reported problems with their radio communication systems.

In a June 2004 Office of Inspector General report on management of Oak Ridge Reservation radio projects, we identified that the two local Department of Energy management offices, the Oak Ridge Office and the Y-12 Site Office, were developing separate radio communication projects. We found that the two projects, as designed, would have created gaps in radio coverage and prevented Y-12 protective forces from maintaining communications with the rest of the Reservation and their own dispatcher in the event of an emergency.

In response to the report, management informed us that work on the separate radio system for the Y-12 Complex had been suspended.

These findings were similar to an earlier review at four other Department sites. During that review, we found that three of the four sites did not have direct radio communications with local law enforcement agencies that would have been called upon to assist in the pursuit of suspected felons or terrorists fleeing Department sites.

Implementation of the Design Basis Threat

The Office of Inspector General has undertaken a three-step process to review the Department's security programs and its progress in meeting the threat posed in the

revised Design Basis Threat (DBT) document. The DBT identifies the potential security threats to Department assets. As a first component in this strategy, we will be completing a review in the near future to determine whether the Department's National Nuclear Security Administration sites will implement the revised DBT by the end of Fiscal Year 2006. We will shortly be initiating a review to determine whether the Department's energy, science, and environment sites will meet the same requirement. As a third component to this process, we intend to review security initiatives throughout the Department to determine if all sites will meet the requirements of a subsequent revision to the DBT by the scheduled date of the end of Fiscal Year 2008.

Conclusion

The Department is addressing many security concerns and is doing so at substantial cost. We are concerned that, in a time of severe budget constraints, escalating security costs may force reduced expenditures for mission-related projects and programs. My office will continue to examine the Department's security apparatus, with the goal of providing recommendations to enhance efficiency and effectiveness.

Mr. Chairman and members of the Subcommittee, this concludes my statement. I will be pleased to answer any questions.